

REMARKS

Applicant has amended claims 26, 28, 30-31, and 50, and have cancelled claims 25, 27, 29, and 32-49, during prosecution of this patent application. Applicant is not conceding in this patent application that the subject matter encompassed by said amended and cancelled claims are not patentable over the art cited by the Examiner, since the claim amendments and cancellations are only for facilitating expeditious prosecution of this patent application. Applicant respectfully reserves the right to pursue the subject matter encompassed by said amended and cancelled claims, and to pursue other claims, in one or more continuations and/or divisional patent applications.

Claim 26 has been rewritten in independent form and is otherwise unchanged by being amended herein.

The Examiner objected to the specification.

The Examiner rejected claims 28, 31 and 50 under 35 U.S.C. § 112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner rejected claims 25, 27 and 29 under 35 U.S.C. § 102(e) as allegedly being anticipated by USP Application Publication 2004/0210767 to Sinclair et al., hereinafter Sinclair.

The Examiner rejected claim 26 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2001/0019614 to Madoukh.

The Examiner rejected claim 28 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2005/0114673 to Raikar et al., hereinafter Raikar.

The Examiner rejected claim 30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2002/0091928 to Bouchard et al., hereinafter Bouchard.

The Examiner rejected claim 31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2004/0107212 to Friedrich et al., hereinafter Friedrich.

The Examiner rejected claim 50 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2005/0114673 to Raikar et al., hereinafter Raikar and USP Application Publication 2001/0048025 to Shinn.

Applicant respectfully traverses the specification objection and the § 112, § 102 and § 103 rejections with the following arguments.

Specification Objection

The Examiner objected to the specification.

The Examiner argues: “The abstract of the disclosure is objected to because the references, non-patent document 1 and 2 can simply be incorporated by reference into the specification. There is no need for the use of reference linking as seen on page two of the written description. Correction is required. See MPEP § 608.01(b).”

In response, Applicant respectfully contends that the Examiner’s objection to the abstract based on “non-patent document 1 and 2 can simply be incorporated by reference into the specification” is puzzling, because the abstract does not mention non-patent documents 1 and 2.

In further response, Applicant respectfully contends that the Examiner’s assertion that “[t]here is no need for the use of reference linking as seen on page two of the written description” is also puzzling, because the content of the abstract has no relationship to reference linking in the written description.

Accordingly, Applicant respectfully requests that the objection to the abstract be withdrawn.

35 U.S.C. § 112, Second Paragraph: Claims 28, 31 and 50

The Examiner rejected claims 28, 31 and 50 under 35 U.S.C. § 112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner argues: “As per claim 31, the phrase the first common user ID” renders the claim indefinite. Examiner cannot ascertain the antecedent basis for this term. It could refer back to a first common identifier or be something new. ”

In response, Applicants have amended claim 31 for clarification purposes.

The Examiner argues: “As per claim 28 and 50, the scope of the claim invention is indefinite because of the uncertainty of the phrase "a data size". Examiner cannot ascertain its meaning or whether there is more than one data size because two data sizes are recited. Similarly, "a number" is defined twice.”

In response, Applicant assert that the Examiner appears to be confused, because the Examiner has erroneously isolated “a data size” from what the data size relates to. Claims 28 and 50 each recite two different data sizes, namely “a data size for fingerprint authentication” and “a data size for voice print authentication”, which is clear.

The Examiner argues: “As per claim 50, the scope of the claim is indefinite because the question is raised whether there is one rule or more than one rule. The claim says there is at least one rule, but lists four rules. How can there be as little as one rule yet four rules are listed? An

argument can be made that there must be at least four rules or that it is possible that rule one contains four parts. Clarification is needed to properly define the metes and bounds of the claim. Specifically whether there is more than one rule or if one rule contains all four limitations as claimed.”

In response, Applicants have amended claim 50 for clarification purposes.

Accordingly, Applicant respectfully requests that the rejection of claims 28, 31 and 50 under 35 U.S.C. § 112, second paragraph be withdrawn.

35 U.S.C. § 102(e): Claims 25, 27 and 29

The Examiner rejected claims 25, 27 and 29 under 35 U.S.C. § 102(e) as allegedly being anticipated by USP Application Publication 2004/0210767 to Sinclair et al., hereinafter Sinclair.

Since claims 25, 27, and 29 have been canceled, the rejection of claims 25, 27, and 29 under 35 U.S.C. § 102(e) is moot.

35 U.S.C. § 103(a): Claim 26

The Examiner rejected claim 26 under 35 U.S.C. § 103(a) as allegedly being unpatentable over USP Application Publication 2004/0210767 to Sinclair in view of USP Application Publication 2001/0019614 to Madoukh.

Applicant respectfully contends claim 26 is not unpatentable over Sinclair in view of Madoukh, because Sinclair in view of Madoukh does not teach or suggest each and every feature of claim 26.

For example, Sinclair does not teach or suggest the feature: “wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method” (emphasis added).

The Examiner argues: “As per claim 26, Sinclair teaches that the servers must first trust one another before sharing policies and resources. Sinclair teaches that the two servers could perform mutual authentication (0022). Sinclair stops just short of teaching the use establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method. *Madoukh teaches establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method (0039).* This is one example of mutual authentication that is well known in the art. Substituting known methods in similar system while yielding predictable results is within the capabilities of one of ordinary skill. Therefore the claim is obvious in view of these two references because one

of ordinary skill could have easily substituted a mutual authentication by public key certificate into Sinclair system with predictable results” (emphasis added).

In response, Applicant notes that Madoukh, Par. [0039] recites: “The KEYDB 44 comprises an external disk array with a fault tolerance system for mirrored operation providing superior fault tolerance. The external disk array includes a redundant array of independent disks (RAID) preferably including five (5) disks. The KEYDB is preferably operated at RAID level 5, which provides data striping at the byte level and also stripe error correction information. Each of the key servers 40, 42 is operable to communicate with the KEYDB 44 through IP and utilizing mutual authentication as described above.”

Applicant acknowledges that the preceding quote from Madoukh, Par. [0039] mentions “mutual authentication as described above”. However, Applicant cannot find a disclosure in Madoukh, Par. [0039] or anywhere else in Madoukh of mutual authentication being performed by an exchange of electronic certificates between the first server and the second server.

Based on the preceding arguments, Applicant respectfully maintains that claim 26 is not unpatentable over Sinclair in view of Madoukh, and that claim 26 is in condition for allowance.

35 U.S.C. § 103(a): Claim 28

The Examiner rejected claim 28 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2005/0114673 to Raikar et al., hereinafter Raikar.

Applicants respectfully contend that Sinclair in view of Raikar does not disclose the following feature of claim 28: “wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method”.

In addition with respect to claim 28, Sinclair in view of Bouchard does not disclose the following feature of claim 28: “wherein the at least one rule includes a data size for fingerprint authentication, a data size for voice print authentication, or a combination thereof

Accordingly, claim 28 is not unpatentable over Sinclair in view of Raikar.

35 U.S.C. § 103(a): Claim 30

The Examiner rejected claim 30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2002/0091928 to Bouchard et al., hereinafter Bouchard.

Applicants respectfully contend that Sinclair in view of Bouchard does not disclose the feature: “wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method”.

In addition with respect to claim 30, Sinclair in view of Bouchard does not disclose the following feature of claim 30: “wherein the authentication policy table of the first server further comprises: a server address of each server registered therein; and a relative priority of each server of a group of servers having a same authentication policy in the authentication policy table”.

The Examiner argues: “As per claim 30, Sinclair teaches storing the known other trusted servers in a table. It is inherent that the address or location to those servers is maintained as well in order to communicate with them. Sinclair fails to teach a relative priority of each server of a group of servers having a same authentication policy in the authentication policy table. Bouchard teaches a system in which multiple servers can designate priority to other servers for authentication in order to balance the load of the system (0047). Load balancing in computer networks is well known in the art. Assigning priority to servers is also well known in the art. Combining known methods in the art and yielding predictable results is within the ordinary capabilities of one of ordinary skill in the art. Therefore the claim is obvious in view of the teachings in the two references. One of ordinary skill could have maintained a priority list to

balance the load of the network. If all the servers are able to perform authentication, it is obvious that they can share in those duties so that one is not overwhelmed.”

In response, Applicant respectfully asserts that Bouchard, Par. [0047] does not teach that multiple servers can designate priority to other servers for authentication in order to balance the load of the system. Rather, Bouchard, Par. [0047] discloses that a message server is configured to perform a load balancing process which determines a least loaded server capable of servicing an authentication/decryption request.

Applicant maintains that there is no disclosure in Bouchard, Par. [0047] of a server designating a priority to other servers, and there is most certainly no disclosure in Bouchard, Par. [0047] of an authentication policy table comprising both a relative priority of each server and an authentication table that includes a server address of each server.

Accordingly, claim 30 is not unpatentable over Sinclair in view of Raikar.

35 U.S.C. § 103(a): Claim 31

The Examiner rejected claim 31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2004/0107212 to Friedrich et al., hereinafter Friedrich.

Applicants respectfully contend that Sinclair in view of Friedrich does not disclose the following feature of claim 31: “wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method”.

Moreover, there are several additional reasons why claim 31 is not unpatentable over Sinclair in view of Friedrich.

A first additional reason why claim 31 is not unpatentable over Sinclair in view of Friedrich is that Sinclair in view of Bouchard does not disclose the feature: “wherein the authentication policy of the second server is identical to an authentication policy of the first server”.

The Examiner acknowledges: “As per claim 31, Sinclair fails to explicitly teach the authentication policy of the second server is identical to an authentication policy of the first server”.

The Examiner does not allege that Bouchard discloses the preceding feature of claim 31.

Therefore, Sinclair in view of Bouchard does not disclose the preceding feature of claim 31.

A second additional reason why claim 31 is not unpatentable over Sinclair in view of Friedrich is that Sinclair in view of Bouchard does not disclose the feature: "wherein a first common user identifier (ID) exists in an authentication information Lightweight Directory Access Protocol (LDAP) of the first server and in an authentication information LDAP of the second server, wherein the first common user ID is used by a first user in the first server and by a second user in the second server such that the second user differs from the first user".

The Examiner argues: "As per claim 31, Sinclair fails to explicitly teach ... wherein a first common identifier (ID) exists in an authentication information Lightweight Directory Access Protocol (LDAP) of the first server and in an authentication information LDAP of the second server, wherein the first common user ID is used by a first user in the first server and by a second user in the second server such that the second user differs from the first user. ... In Sinclair's system, multiple servers pool together their known authentication policies including those users belonging to each server. It is not unreasonable for one of ordinary skill to consider what would happen in the same user ID existed in both groups. LDAP which is notoriously well known in the art and taught by Friedrich, handles this occurrence through home repositories which are unique to each user even if the user name is common. Friedrich addresses this situation by maintaining the home repository of each user in conjunction with a unique identifier (probably the SID or some other unique attribute to the user) (0033). This solves the problem of common user names by creating a pointer to which server or repository that user belongs to. In view of this teaching, Examiner finds that claim is obvious because one of ordinary skill could have first recognized the potential for two users having a common user name and dealt with it in the means taught by Friedrich."

In response, Applicants respectfully contend that Friedrich, Par. [0033] teaches explicitly that the first common user ID does not exist in both the authentication information LDAP of the first server and the authentication information LDAP of the second server as required by the preceding feature of claim 31. Specifically, Friedrich, Par. [0033] recites: “objects with the same identifier cannot exist in different adapters/repositories (e.g., the system does not support situations where the same user ID is stored in two different LDAP repositories).”

Therefore, Sinclair in view of Bouchard does not disclose the preceding feature of claim 31.

A third additional reason why claim 31 is not unpatentable over Sinclair in view of Friedrich is that Sinclair in view of Bouchard does not disclose the feature: “after said registering the authentication policy of the second server, registering by the first server the first common user ID in an exceptional ID table of the first server, wherein the exceptional ID table of the first server stores common user IDs and an indication of one or more servers associated with each common user ID stored in the exceptional ID table of the first server”.

The Examiner has not presented any argument allegedly demonstrating that Sinclair in view of Bouchard does not disclose the preceding feature of claim 31.

Therefore, Sinclair in view of Bouchard does not disclose the preceding feature of claim 31.

Accordingly, claim 31 is not unpatentable over Sinclair in view of Friedrich.

35 U.S.C. § 103(a): Claim 50

The Examiner rejected claim 50 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Sinclair in view of USP Application Publication 2005/0114673 to Raikar et al., hereinafter Raikar and USP Application Publication 2001/0048025 to Shinn.

Applicants respectfully contend that Sinclair in view of Raikar and Shinn does not disclose the following feature of claim 50: “wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method”.

In addition with respect to claim 50, Sinclair in view of Bouchard does not disclose the feature: “wherein the at least one rule consist of four rules, said four rules consisting of a number of alphabetic characters of a user identification (ID), a number of numeric characters of the user ID, a data size for fingerprint authentication, and a data size for voice print authentication”.

The Examiner argues: “As per claim 50, Sinclair teaches that password policies and parameters are maintained in a database (0025). However, Sinclair fails to elaborate that the parameters include a number of alphabetic characters of a user identification (ID), a number of numeric characters of the user ID, a data size for fingerprint authentication, a data size for voice print authentication. Raikar teaches using strong passwords which include a combination of a number of alphabetic characters of a user identification (ID), a number of numeric characters of the user ID (0037). Shinn teaches the use of a biometric template used in authenticating fingerprints and voice prints (0033). Each of these teaching provides a secure means to manage a network. Specifically they teach a way to improve the security of the system by creating strict measures to enforce user authentication into the system and prevent unauthorized access.

Therefore the claim is obvious in view of these three references because one of ordinary skill could have easily substituted a combination of password parameters and biometric templates as taught by Raikar and Shinn, respectively, into Sinclair system with predictable results. Based on the interpretation of the claim stemming from its lack of definitiveness, Examiner finds the rule belonging to the each user ID references not the user ID itself but the password associated with the User ID.”

In response, Applicant notes that Shinn, Par. [0019] recites: “The biometric template includes at least one model of biometric patterns for the user, such as the user's voice print, ... , fingerprint, ...”. However, Shinn does not disclose “*a data size* for fingerprint authentication” and “*a data size* for voice print authentication”. Instead, Shinn, Par. [0019] recites “The information fields also include a table of *pre-defined probability of occurrence values* for user authentication”.

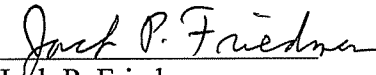
In further response, Applicant respectfully contends that Sinclair in view of Raikar and Shinn does not disclose the preceding feature of claim 50 in light of the closed ended limitation of “*consisting of* a number of alphabetic characters of a user identification (ID), a number of numeric characters of the user ID, a data size for fingerprint authentication, and a data size for voice print authentication”.

Accordingly, claim 50 is not unpatentable over Sinclair in view of Raikar and Shinn.

CONCLUSION

Based on the preceding arguments, Applicant respectfully believes that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicant invites the Examiner to contact Applicant's representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account 09-0457 (IBM).

Date: 03/04/2009


Jack P. Friedman
Registration No. 44,688

Customer No. 30449
Schmeiser, Olsen & Watts
22 Century Hill Drive - Suite 302
Latham, New York 12110
Telephone (518) 220-1850
Facsimile (518) 220-1857
E-mail: jfriedman@iplawusa.com